REMARKS/ARGUMENTS

The present amendment is responsive to the Office Action dated January 16, 2007. Claims 1, 11, 21 and 31 have been amended. No new matter has been introduced by these amendments. Claims 45-46 have been cancelled in view of the Office Action maintaining the restriction of these claims. Claims 2-5, 12-15, 22-25 and 32-35 were previously canceled. Therefore, claims 1, 6-11, 16-21, 26-31, and 36-44 are again presented for consideration in view of the following remarks. A petition for a one-month extension of time is submitted herewith.

As noted above, the Office Action maintained the withdrawal of claims 45-46 as being "beyond the scope of the previously claimed subject matter." (Office Action, pg. 3.) These claims have been cancelled, and applicants reserve the right to file a divisional application directed to these claims.

Claims 1, 6-11, 16-21, 26-31, and 36-44 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,862,220 ("*Perlman*") in view of U.S. Patent No. 6,049,671 ("*Slivka*"). Claims 1, 6-11, 16-21, 26-31, and 36-44 were also rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,182,142 ("*Win*") in view of *Slivka*. Applicants respectfully traverse both grounds of rejection. As all claims were rejected in both grounds, the rejections will be addressed together.

Claim 1 has been amended to recite "A method of transmitting data from a transmission apparatus to one of a plurality of receiving terminals, comprising: communicating between said one receiving terminal and the transmission apparatus via an Internet system, said one receiving terminal being operable to receive a digital broadcasting signal;

receiving authentication data associated with said one receiving terminal; authenticating said authentication data; transmitting unique terminal information identifying said one receiving terminal as a destination of transmission and an update program to change the processing of said one receiving terminal, said unique terminal identification information being selected in a manner unrelated to said authentication data, and said transmitting step including converting said unique terminal information into converted unique terminal information comprising a key ID and transmitting said converted unique terminal information to said one receiving terminal; at said one receiving terminal comparing the transmitted key ID to an assigned key ID generated at the receiving terminal to determine whether the transmitted key ID and the assigned key ID are identical; and upon determining that the transmitted key ID and the assigned key ID are identical: updating the processing of said one receiving terminal, said updating step including receiving at said one receiving terminal said unique terminal information and said update program; returning said converted unique terminal information comprising a key ID to said unique terminal information; storing said unique terminal information and said update program in a storage location after said returning step; transmitting from said one receiving terminal to said transmission apparatus a transfer request based on said update program and said unique terminal information; and supplying data responsive to said transfer request from said transmission apparatus to said one receiving terminal based on said unique terminal information."

Independent claim 11 has been amended to include "wherein said unique terminal identification information is selected in a manner unrelated to said authentication data, said transmission apparatus transmits said unique terminal information converted into a key ID to said one receiving

terminal, and said one receiving terminal compares the transmitted key ID to an assigned key ID generated at the receiving terminal to determine whether the transmitted key ID and the assigned key ID are identical, and upon determining that the transmitted key ID and the assigned key ID are identical, said one receiving terminal converts said converted unique terminal information back to said unique terminal information and then stores said unique terminal information in said storage location."

Independent claim 21 has been amended to include "wherein said one receiving terminal compares the received key ID to an assigned key ID generated at the receiving terminal to determine whether the received key ID and the assigned key ID are identical, and upon determining that the received key ID and the assigned key ID are identical, said one receiving terminal is operable to store said unique terminal information and said update program and to generate said transfer request."

And independent claim 31 has been amended to recite "A method of receiving data transmitted from a transmission apparatus to one of a plurality of receiving terminals, comprising: communicating between said one receiving terminal and the transmission apparatus via an Internet system, said one receiving terminal being operable to receive a digital broadcasting signal; receiving unique terminal information identifying said one receiving terminal as a destination of transmission and an update program for changing the processing of said one receiving terminal, said unique terminal identification information being selected in a manner unrelated to authentication data associated with said one receiving terminal; converting said unique terminal information into a key ID; at said one receiving terminal comparing a received key ID directly associated with said received unique terminal

information to an assigned key ID generated at the receiving terminal to determine whether the received key ID and the assigned key ID are identical; and upon determining that the transmitted key ID and the assigned key ID are identical: storing said unique terminal information and said update program received by said one receiving terminal in a storage location; transmitting said unique terminal information and a transfer request based on said update program from said one receiving terminal to said transmission apparatus; and receiving data transmitted from said transmission apparatus in response to said transfer request based on said unique terminal information."

Support for these amendments may be found, by way of example only, at pages 9-14 of the specification as filed, as well as in FIG. 5.

Features of *Perlman* and *Slivka* and specific deficiencies of these references have been addressed in detail in the responses to prior Office Actions. These analyses are fully incorporated by reference herein for the sake of brevity.

Win is directed to a system for controlling access to information resources on a distributed network. According to the Abstract, a "runtime module on the protected server receives the login request and intercepts all other request by the client to use a resource. The runtime module connects to an access server that can determine whether a particular user is authentic and which resources the user is authorized to access." Furthermore, the "access server passes encrypted tokens that define the user's roles and authorization rights to the browser or client, which stores the tokens in memory." (Abstract.) This results in presenting the user "with a customized display showing only those resources that the user may access." (*Id.*)

Win illustrates various state diagrams in FIGS. 5A-5E

to show steps carried out in verification, login processing, user profile generation, logout processing and personalized menu generation. As explained in *Win* with regard to FIG. 5C,

> FIG. 5C is a state diagram of actions taken by the browser, Registry Server 108, and Access Server 106 when a user is authenticated. After a user is authenticated, the Authentication Client module 414 calls the Authorization service of Access Server 106. In response, the Authorization service requests profile information about the user from the Registry Server 108, as shown by state 520. In state 522, Registry Server 108 returns the profile information to Access Server 106. The profile information may comprise the user's name, locale information, IP address, and information defining roles held by the user. The Authorization service creates a "user cookie" 528 and "roles cookie" 530, which are used to convey profile information to browser 100. The "user cookie" contains a subset of the user profile information. The "roles cookie" contains a list of the user's roles.
>
> As shown by state 524, cookie 528 and cookie 530 are encrypted and returned to the browser 100. Alternatively, state 524 may involve digitally signing cookie 528 and cookie 530 using a digital signature algorithm. Preferably, the cookies are encrypted rather than digitally signed because encryption is faster and produces a smaller cookie. Each of the cookies 528, 530 is marked with or contains an expiration date value.
>
> Cookie 528 and cookie 530 are saved in memory by the browser 100 indefinitely, unless either of the cookies expires, i.e., the system clock becomes equal to or greater than the expiration date value. The cookies 528, 530 are passed to each Web server that the user accesses and that is within the same domain as the Access Server 106. When a user quits the browser 100, cookies that have not expired are saved on a mass storage device associated with the browser 100, such as a disk drive located at the user's client machine or terminal. Cookies that have an expiration date value of 0 are never saved on disk. Administrators can apply security policies to the system by setting cookie expiration times based on their organization's security policies.

(Col.10, l.53 to col.11, l.21.)

In *Win*, there is a comparison between passwords by the Registry Server, which is explained as follows:

> Access Server 106 asks Registry Server 108 to verify the user's password. Passwords are stored in the Registry Server 108 in an encrypted format. The Registry Server 108 compares passwords and returns the result. If the password is correct, Access Server 106 encrypts data in a User cookie 528 and Roles cookie 530. Cookies are encrypted rather than digitally signed because encryption is faster and produces a smaller cookie, both factors that result in better performance.
>
> (Col.23, ll.32-40.)

However, while cookies may be saved in memory by a browser and passwords may be compared elsewhere in the system, such features are not what is claimed. For instance, independent claims 1 and 11 each require a comparison of the transmitted key ID to an assigned key ID generated at the receiving terminal to determine whether they are identical. And claims 21 and 31 each require a comparison of the received key ID to an assigned key ID generated at the receiving terminal to determine whether they are identical. As claimed, the comparisons occur at the receiving terminal.

Only upon determining that the two key IDs are identical do certain actions occur at the receiving terminal. By way of example only, in claim 1, after the determination is made, the steps of returning, storing, transmitting and supplying may occur. In claim 11, upon determining that the key IDs are identical, the receiving terminal converts the converted unique terminal information back to said unique terminal information and then stores said unique terminal information in said storage location. In claim 21, once the determination is

made, the receiving terminal is operable to store the unique terminal information and the update program and is also operable to generate the transfer request. And in claim 31, once the determination is made, the steps of storing, transmitting are receiving may occur.

Slivka does not overcome the deficiencies of *Win*. Furthermore, the applied combination of *Perlman* and *Slivka* also fails to teach or suggest each and every limitation of the independent claims.

Thus, applicants respectfully submit that the combinations of *Perlman* and *Slivka* and *Win* and *Slivka* as applied in the rejections do not disclose or otherwise suggest all features as claimed. For at least this reason, applicants submit that independent claims 1, 11, 21 and 31 are in condition for allowance.

Claims 6-10, 16-20, 26-30 and 36-44 depend from claims 1, 11, 21, and 31, respectively, and contain all the limitations thereof. Accordingly, applicants submit that the subject dependent claims are likewise patentable.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: May 14, 2007

Respectfully submitted,

By _____

Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

732921_1.DOC